Introduction to the Electronic Signatures Law of People's Republic of China

MINYAN WANG AND MINJU WANG

This introduction provides the legislative background of the Electronic Signatures Law in China, and aims to briefly introduce and explain the content of this law to facilitate the understanding of the translation of this law.

The Legislative background of the Electronic Signatures Law

Although there have been few cases on electronic commerce before to the courts in China,[1] the debate on regulating electronic commerce is intense in China. The first relevant regulation on electronic commerce traces back to the Contract Law issued in March 1999. Article 11 of the Contract Law provides that:

> "A writing means a memorandum of contract, letter or data message (including telegram, telex, facsimile, electronic data exchange and electronic mail), etc. which is capable of presenting its contents in a tangible form."

That means the data message is recognized as a form of writing in law. Article 16 concerns about the time of contract formation, which provides that:

> "An offer becomes effective when it reaches the offeree. When a contract is concluded by the exchange of data messages, if the recipient of data messages has designated a specific system to receive it, the time when data messages enter into such specific system is deemed the time of arrival; if no specific system has been designated, the time when the data messages first enter into any of the recipient's systems is deemed the time of arrival."

Article 34 concerns about the place of contract formation, which provides that:

> "The place where the acceptance becomes effective is the place of formation of a contract. Where a contract is concluded by the exchange of data messages, the recipient's main place of business is the place of formation of the contract; if the recipient does not have a main place of business, its habitual residence is the place of formation of the contract. If the parties have agreed otherwise, such agreement prevails".

However, the Contract Law only recognizes the data message as a form of writing, it does not prescribe how a data message fulfills the legal requirement of originality, retention and admissibility as an evidence, amongst other things.

The following years saw the introduction of some regulations, for example, the Telecommunication Ordinance 2000, the Internet Information Service Administration Measure 2000, the Copyright Law 2001 and some local governments regulations. However, the majority of these regulations are local or departmental, and they are mostly concerned with information security, information administration, intellectual property, or system infrastructure. Issues such as electronic signatures, transaction rules, consumer protection and legal liability are not dealt with. Therefore, it is said that the Electronic Signatures Law is the first national e-commerce legislation in China.

In fact, electronic signatures have been utilized in electronic commerce before the Electronic Signatures Law was enacted. In some cities, such as Shanghai, Beijing, Guangzhou, Shenzhen, Hainan, the certification authorities (CAs) were set up to provide certification services.[2] The China Financial Certification Authority (CFCA, 2000)[3] was set up by twelve banks, including the People's Bank of China, to provide certification service to its

In fact, electronic signatures have been utilized in electronic commerce before the Electronic Signatures Law was enacted

[1] This information came from a speech by Judge Hongguang Wang, the Super Court in China at a public forum.
[2] It is said there are about 80 CAs in China. This information comes from http://tech.sina.com.cn/it/2004-08-25/1019411791.shtml.
[3] See http://www.cfca.com.cn

clients. Some local governments also tried to regulate and administrate the certification services. For example, Shanghai, Guangdong, Hainan and Liaoling Province have released the rules on digital signatures.[4]

Since electronic commerce plays a more important role in economic development, and in an effort to standardise the practice of CAs, and to clarify the legal validity of e-record or e-document, the State Council's Informationalization Office decided to enact the Electronic Signatures Ordinance of People's Republic of China in 2002, which was thought to be an administrative regulation. However, when the Informationalization Office submitted the Ordinance to the State Council's Legislative Affairs Office in 2003, the Legislative Affairs Office, taking into account the importance of e-documents and e-records in electronic commerce and the fast development of electronic commerce, decided to enact an electronic signatures law instead of an ordinance. As a result, the draft Electronic Signatures Law was submitted to the State Council on 25 March 2004. On 28 August 2004, the Electronic Signatures Law was Passed by No. 11 meeting of the No. 10 Standard Committee of the National People's Congress, and it will come into force on 1 April 2005.

The brief content of the Electronic Signatures Law

The Electronic Signatures Law consists of five chapters – general articles, data message, electronic signatures and recognition, legal liability, and supplementary articles, from which one might be aware that the law does not merely deal with electronic signatures, but also data messages. Chapter one states the legislative purpose and sphere of application, defines the 'electronic signature' and 'data message' and recognizes the legal effects of data messages and electronic signatures. Chapter two is "Data Message", which is concerned with the writing requirements, the original requirements, admissibility and evidential weight of data messages, retention of data messages, acknowledgement of receipt, attribution of data messages, time and place of dispatch and receipt of data messages. Chapter three refer to "electronic signatures and recognition", which deals with the reliable electronic signature, conduct of the signatory, conduct of the certification authorities, etc. Chapter four is "legal liability", concerning the liability of the conduct of the signatory, the relying party and the certification authorities. Chapter five provides some definitions and interpretations.

Main features of the Electronic Signatures Law

First, the Electronic Signature Law recognizes the legal validity of data messages and electronic signatures. The document shall not be denied legal effect on the sole ground that it is in the form of a data message or that an electronic signature is used.[5] However, data messages and electronic signatures shall not be applied to the documents in connection with the personal relationship, transfer of interests in real estate, and suspension of public utility services.[6]

Second, the Electronic Signatures Law adopts a "functionally equivalent approach" when evaluating the legal effects of data messages and electronic signatures. If those purposes or functions of writing or signature could be achieved by data messages or electronic signatures, that data messages or electronic signatures enjoys the same level of legal recognition as the paper-based documents or handwritten signatures or seals.[7]

Third, the approach to regulate electronic signatures adopted by the Electronic Signatures Law is technology-neutral one. The electronic signatures refer to various techniques.[8] No matter what kinds of technologies are utilized in an electronic signature, the law provides the legal recognition of electronic signatures.[9] However, from the expression of article 13, it seems that only the digital signature is considered to be a reliable form of electronic signature.

However, the Electronic Signatures Law merely sets up a legal framework for the electronic environment, and does not cover every aspect of the use of data messages and electronic signatures in electronic commerce. The more detailed and comprehensive implementing rules and administrative regulations are needed to supplement the Electronic Signatures Law, which are under several local governments' agenda now and will come out in the near future. ■

Minyan Wang
LL.B(Hons)(East China University of Politics & Law, PRC), LL.M (University of Manchester), Ph.D Candidate (Queen Mary, University of London) Centre for Commercial Law Studies, Queen Mary, University of London and the China Correspondent to the e-Signature Law Journal.

m.wang@qmul.ac.uk

Minju Wang
LL.B (East China University of Politics & Law, PRC)
Legal Consultant, Xiamen Ya-Li-Sheng Co. Ltd. P.R.China

xmwmj@hotmail.com

[4] For example, on 6th December, 2002 Guangdong province passed the Electronic Transactions Regulations, which became effective as of 1st February, 2003, available in electronic format at: http://www.sol.net.cn/law/law_show.asp?ArticleID=20344.
[5] Article 3.
[6] Article 3.
[7] Article 4, 5, 6 and 14.
[8] Article 2.
[9] Article 13.

Unofficial translation of the Electronic Signatures Law of the People's Republic of China of 28 August 2004 by Minyan Wang and Minju Wang

Electronic Signatures Law of People's Republic of China
Passed by No. 11 meeting of No. 10 Standard Committee of the National People's Congress on 28 August, 2004

Content:

Chapter 1: General Articles
Article 1: To standardise the behavior of electronic signatures, to recognize the legal validation of electronic signatures and to protect the legitimate rights and interests of the relevant parties, the law was enacted.

Article 2: "Electronic signature" in this law means data in electronic form in or affixed to a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.
"Data message" means information generated, sent, received or stored by electronic, optical, magnetic or similar means.

Article 3: The parties may stipulate whether or not to use an electronic signature or a data message in contracts or other documents in the context of civil activities.
Where the parties stipulate the use of an electronic signature or a data message in a document, that document shall not be denied legal effect on the sole ground that it is in the form of an electronic signature or a data message.
The aforesaid paragraphs shall not be applied to the following documents:
(1) In connection with marriage, adoption, heritage or other personal relationship;
(2) In connection with transfer of interests in real estate such as land and dwelling;
(3) In connection with suspension of public utility services such as water, heat, gas and electricity;
(4) As otherwise provided by laws and regulations.

Chapter 2: Data Message
Article 4: A data message which is capable of presenting the information contained tangibly and is accessible for use and investigation at any moment shall be deemed to be in writing as required by the laws and regulations.

Article 5: A data message shall be deemed to be in its original form as required by laws and regulations where it satisfies the following requirements:
(1) It can present the information contained effectively and is accessible for use and investigation at any moment;
(2) There exists a reliable assurance that the information has remained complete and unaltered from the time when its final form was first generated. However, the addition of any endorsement and any changes that may arise in the course of communication, storage or display of data does not affect the integrity of the data message.

Article 6: A data message shall be deemed to be retained as required by the laws and regulations where it satisfies the following requirements:

(1) It can present the information contained effectively and is accessible for use and investigation at any moment;
(2) The data message is retained in the same format in which it was generated, transmitted or received, or if in a different format it can represent accurately the information generated, transmitted or received;
(3) It can identify the originator and recipient of a data message and the date and time of its dispatch and receipt.

Article 7: A data message shall not be denied being admitted as evidence on the sole ground that it is generated, sent, received, stored by electronic, optical, magnetic or similar means.

Article 8: In assessing the evidential weight of a data message, the following factors shall be taken into account:
(1) The reliability of the manner in which the data message was generated, stored or transmitted;
(2) The reliability of the manner in which the integrity of the information therein was maintained;
(3) The reliability of the manner in which its originator was identified;
(4) Any other relevant factors.

Article 9: A data message is deemed to be sent by the originator if any of the following conditions has been met:
(1) It was sent under the authorization of the originator;
(2) It was sent automatically by the originator's information system;
(3) The addressee verifies and ascertains the data message by a method ratified by the originator.
If the parties have agreed otherwise, such agreement prevails.

Article 10: Where the laws and regulations require or the parties agree that receipt of a data message be acknowledged, the receipt shall be acknowledged. When the originator receives the addressee's acknowledgement of receipt, the data message is deemed to be received by the addressee.

Article 11: The time when a data message enters an information system outside the control of the originator is deemed to be the time that data message is sent.
Where the addressee has designated an information system for the purpose of receiving a data message, the time when the data message enters the designated information system is deemed to be the time of receipt of the data message; if the addressee has not designated an information system, the time when the data message first enters any information system of the addressee is deemed to be the time of receipt of the data message.
If the parties agree otherwise on the time of dispatch and receipt, such agreement prevails.

Article 12: The originator's principal place of business is deemed to be the place where a data message is dispatched. The addressee's principal place of business is the place where a data message is received. If the originator or the addressee does not have a principal place of business, reference is to be made to its habitual residence.
If the parties have agreed otherwise on the place of dispatch and receipt, such agreement prevails.

Chapter 3: Electronic Signatures and Recognition
Article 13: An electronic signature is deemed to be a reliable electronic signature if the following requirements are met:
(1) The signature creation data, when used to an electronic signature, is linked to the signatory and to no other person;
(2) The signature creation data is under the control of the signatory and of no other person when signing;
(3) Any alteration to an electronic signature, made after the time of signing, is detectable;
(4) Any alteration to the content or form of a data message, made after the time of signing, is detectable.
The parties may choose the form of electronic signature that meets the agreed reliability requirements.

Article 14: The reliable electronic signature has the same legal effect as the hand-written signature or seal.

Article 15: The signatory shall exercise reasonable care to protect the signature creation data. If the signatory knows that the signature creation data has been compromised or may have been compromised, he shall notify any related party without undue delay and stop using the signature creation data.

Article 16: Where electronic signature requires recognition by a third party, it is the certification service provider established in accordance with the law that provides the certification service.

Article 17: To provide the certification service, the following requirements shall be met:
(1) It shall have professional technical and management personnel qualified to provide the electronic certification services;
(2) It shall have sufficient capital funds and an operational site that is appropriate to its corresponding electronic certification services;
(3) It shall have technologies and equipment that meet national security standards;
(4) It shall obtain a certificate verifying that the national cryptogram administrative institute agrees it to use cryptogram;
(5) Other requirements as prescribed by the laws and regulations.

Article 18: To provide the certification service, an applicant shall apply to the Ministry of Information Industry of the State Council and submit the relevant documents in accordance with Article 17 of this law. The Ministry of Information Industry of the State Council shall examine the application according to the law when receiving the application, solicit to the Ministry of Commerce or other relevant ministries of the State Council, and then decide whether to issue a licencing or refuse to issue a licence within forty-five days after the application is received. If a licence is issued, the Ministry of Information Industry shall issue the licence of the certification service; if a licence is refused, the Ministry then shall inform the applicant and provide reasons for refusing in writing.
The applicant shall register with the Administrative Authority of Industry and Commerce according to the law, together with the electronic certification license.
The certification service provider holding the licence of the certification service shall publish its title, the licence number and other information on the website required by the Ministry of Information Industry of the State Council.

Article 19: The certification service provider shall formulate and publish the code of practice with respect to electronic certification business in accordance with the law, and put the Code on record with the Ministry of Information Industry of the State Council.
The code of practice on electronic certification business shall include the scope of liability, operation standards, information security safeguard measures or other related matters.

Article 20: Where a signatory applies to the certification service provider for a certificate, he shall provide genuine, complete and accurate information.
When the certification service provider receives the application for the certificate, he shall examine the applicant's identity and review the relevant materials.

Article 21: The certificate issued by the certification service provider shall be accurate and record the following information:
(1) The name of the certification service provider;
(2) The name of the certificate holder;
(3) The certificate serial number;
(4) The validation period of the certificate;
(5) The certificate holder's electronic signature verification data;
(6) The electronic signature of the certificate service provider;

(7) Other information required by the Ministry of Information Industry of the State Council.

Article 22: The certification service provider shall ensure the information contained in the certificate, within the validation period of the certificate, is complete and accurate, and ensure that a relying party could ascertain and understand the information contained in the certificate and other relevant matters.

Article 23: The certification service provider who intends to suspend or terminate the certification service shall inform the relevant parties on takeover of the business and other relevant matters ninety days before the service is suspended or terminated.
The certification service provider who intends to suspend or terminate the certification service shall notify the Ministry of Information Industry of the State Council sixty days before the service is suspended or terminated, and negotiate with other certification service providers to take the business over and make the appropriate arrangements.
If the certification service provider cannot make an agreement with any other certification service providers to take the business over, he shall apply to the Ministry of Information Industry of the State Council for arranging other certification service providers to take over his business.
Where the licence of the certification service provider to provide the electronic certification service is suspended according to the law, the business will be taken over in accordance with the provisions prescribed by the Ministry of Information Industry of the State Council.

Article 24: The certification service provider shall duly retain all the information in connection with the electronic certification for a minimum period of five years after the expiration date of the certificate.

Article 25: The Ministry of Information Industry of the State Council enacts the provisions on administration of the certification service, supervises and administrates the certification service providers in accordance with the law.

Article 26: Subject to the verification by the Ministry of Information Industry of the State Council according to the relevant agreement or the reciprocity principle, the certificate issued outside the People's Republic of China by a foreign certification service provider shall have the same legal effect as the certificate issued by the certification service provider established in accordance with this law.

Chapter 4: Legal liability

Article 27: Where the signatory knows that the signature creation data has been compromised or may have been compromised, but fails to notify the relevant parties without undue delay and to cease to utilize the signature creation data, or where the signatory does not provide genuine, complete and accurate information to the certification service provider, or is responsible for any other faults, he shall be responsible for any damages suffered by the relevant relying parties and the certification service provider.

Article 28: Where a signatory or relying party suffers damages when acting in its civil activities based on the electronic certification services provided by the certification service provider, the certification service provider shall be responsible for relevant damages if it fails to prove it is not at fault.

Article 29: Where someone provides electronic certification service without a valid licence, the Ministry of Information Industry of the State Council shall order the termination of the illegal activities; any income from the illegal activities shall be confiscated; in case of the illegal income exceeding 300,000 yuan, a fine of 1 to 3 times of the income shall be imposed; in case of no illegal income or the income less than 300,000 yuan, a fine of 100,000 to 300,000 yuan shall be imposed.

Article 30: If the certification service provider suspends or terminates the certification service, but fails to notify the Ministry of Information Industry of the State Council sixty days before the service is suspended or terminated, the Ministry of Information Industry of the State Council shall impose a fine of 10,000 to 50,000

yuan on the director directly responsible for the matter.

Article 31: Where the certification service provider does not comply with the rules applicable to the certification service, fails to save and recognize the relevant information appropriately, or commits other illegal activities, the Ministry of Information Industry of the State Council shall order to correct the act within a specified time; if it is not corrected within the specified time, the licence of the certification service shall be suspended, and the director directly responsible for the matter and any other personnel with a direct responsibility will not be permitted to engage in the certification service for a period of ten years. If the licence of certification service is suspended, a public notice shall be given and the Administration Authority of Industry and Commerce shall be informed.

Article 32: If there is forgery, infringement or fraudulent use of electronic signatures, in case of constituting a crime, the criminal responsibilities shall be investigated and imposed in accordance with the law; if there is damage suffered by others, the civil liabilities shall be imposed in accordance with the law.

Article 33: If the missionary in the department responsible for the supervision and administration of the certification service according to this law does not perform the duty of administrative licence, supervision and administration according to the law, the administrative sanction shall be imposed in accordance with the law; in case of constituting a crime, the criminal responsibilities shall be investigated and imposed in accordance with the law.

Chapter 5: Supplementary Articles

Article 34: For the purpose of this law the following words will have the meanings set out below:

(1) "Signatory", means a person that holds signature creation data and acts on its own behalf or on behalf of the person it represents;
(2) "Relying party", means a person that may act in reliance on a certificate or an electronic signature;
(3) "Certificate", means a data message or other record confirming the link between a signatory and signature creation data;
(4) "Signature creation data", means data such as keys and codes that reliably link the electronic signature with the signatory in the making of such electronic signature;
(5) "Electronic signature verification data", means a data used to verify an electronic signature, including code, password, algorithm and the public key, etc.

Article 35: The State Council or the ministry prescribed by the State Council may enact the provisions regarding the usage of electronic signatures and data messages in the governmental activities or other social activities according to this law.

Article 36: This law will come into force on 1 April, 2005.